

# ANÁLISES COMPUTACIONAIS PREDITIVAS COMO UM NOVO BIOPODER: MODIFICAÇÕES DO TEMPO NA SOCIEDADE DOS SENSORES

PREDICTIVE ANALYTICS AS A NEW BIOPOWER: TIME CHANGES IN THE  
SOCIETY OF SENSORS

ANÁLISIS COMPUTACIONALES PREDICTIVOS COMO UN NUEVO  
BIOPODER: MODIFICACIONES DEL TIEMPO EN LA SOCIEDAD DE LOS  
SENSORES

#### Licença CC BY:

Artigo distribuído sob os termos Creative Commons, permite uso e distribuição irrestrita em qualquer meio desde que o autor credite a fonte original.



Elias Jacob de Menezes Neto<sup>1</sup>  
Jose Luis Bolzan de Moraes<sup>2</sup>

**Resumo:** O objetivo deste artigo é analisar o surgimento dos mecanismos de análises preditivas associados à *big data*. Primeiro, apresentamos uma introdução ao conceito de "sociedade dos sensores", que viabiliza a coleta de grandes quantidades de dados constantemente. Estes dados são o fundamento dos algoritmos de análises preditivas, sendo problemáticos para o direito, pois tais análises possibilitam que seres humanos sejam categorizados com base nos resultados de um conjunto complexo de algoritmos que não podem ser explicados de modo tradicional. Por fim, retomamos ao conceito de biopoder de Foucault, argumentando que se trata de um modelo útil para pensar o poder no cenário exposto, desde que devidamente atualizado. Concluímos que o biopoder agora é híbrido, vez que congrega uma diversidade enorme de tecnologias, sempre com a finalidade de identificar e rastrear indivíduos e grupos, bem como criar modelos preditivos de comportamento e risco.

**Palavras-chave:** Sociedade dos sensores; Direitos humanos; Análises de *big data*.

- 1 Mestre e Doutor em Direito Público pela Universidade do Vale do Rio dos Sinos. Professor adjunto do curso de Direito da Universidade Federal do Rio Grande do Norte, *campus* de Caicó/RN. Coordenador do Núcleo de Prática Jurídica e do Laboratório de Governança Pública, ambos da UFRN. E-mail: eliasjacob@ceres.ufrn.br.
- 2 Mestre em Direito pela Pontifícia Universidade Católica do Rio de Janeiro. Doutor em Direito pela Universidade Federal de Santa Catarina. Bolsista de Produtividade em Pesquisa do CNPq – Nível 1D. Professor do Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – Mestrado e Doutorado. E-mail: bolzan@hotmail.com.

**Abstract:** This paper analyzes, from a socio-legal perspective, the emergence of big data predictive analytics. Initially, we present the idea of a "sensor society", which enables the collection of large amounts of data all the time, and which is the basis for big data analytics. From a legal perspective, they pose a threat to human rights, because they enable the creation of categories such as "risk" as the result of a complex set of algorithms that cannot be explained by human reasoning. Finally, we return to Foucault's concept of biopower, arguing that it is a useful model for thinking about power in this scenario, provided it is properly updated. We conclude that biopower is now a hybrid, since it is made of a plethora of technologies that have the common purpose of identifying and tracking individuals and groups in order to create predictive models of behavior and risk.

**Keywords:** Sensors society; Human rights; Big data analytics.

**Resumen:** El objetivo de este artículo es analizar el surgimiento de los mecanismos de análisis predictivos asociados al big data. Primero, presentamos una introducción al concepto de "sociedad de los sensores", que viabiliza la colecta de grandes cantidades de datos constantemente. Estos datos son el fundamento de los algoritmos de análisis predictivos, siendo problemáticos para el derecho, pues tales análisis posibilitan que seres humanos sean categorizados con base en los resultados de un conjunto complejo de algoritmos que no pueden ser explicados de modo tradicional. Por último, retomamos el concepto de biopoder de Foucault, argumentando que se trata de un modelo útil para pensar el poder en el escenario expuesto, siempre que debidamente actualizado. Concluimos que el biopoder ahora es híbrido, que congrega una diversidad enorme de tecnologías, siempre con la finalidad de identificar y rastrear individuos y grupos, bien como crear modelos predictivos de comportamiento y riesgo.

**Palabras-clave:** Sociedad de los sensores; Derecho humanos; Análisis de big data.

## INTRODUÇÃO

No mundo globalizado, existe a necessidade de facilitar, cada vez mais, os fluxos e, simultaneamente, restringi-los. Todavia, esses mesmos fluxos possibilitam o surgimento de um "lado negro" da globalização, caracterizado pela expansão daquilo que Zygmunt Bauman<sup>3</sup> chama de medo líquido (e que deriva, justamente, das incertezas criadas pela interconexão viabilizada pela globalização).

Essas incertezas geram demandas por novos mecanismos prontos para neutralizá-las. Apostamos, então, na criação de modelos de computador preditivos, capazes de antecipar o futuro através de análise matemática de eventos do passado. Por não ser um ramo de amplo conhecimento no mundo jurídico, será feito o amplo uso de exemplos com a finalidade de familiarizar o leitor com a ideia de que, em análises estatísticas e probabilísticas, uma única

3 BAUMAN, Zygmunt. **Medo líquido**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2008. 239 p.

nova informação é capaz de modificar radicalmente o resultado da análise<sup>4</sup>.

Se isso é verdade para uma única informação, não fica difícil imaginar quais seriam as possibilidades de análises com um volume de dados tão grande que nem mesmo os sistemas tradicionais de computação conseguem dar conta, como é o caso do *big data*. Como resultado do barateamento das estruturas de coleta e armazenamento de dados, passaram a surgir novas possibilidades para análises e identificação de padrões em eventos aparentemente aleatórios.

Isto ocorre porque, fora dos limites humanos, técnicas de *big data* trabalham com conjuntos tão grandes de dados que permitem a identificação de correlações que, para um ser humano, parecem desconexas.

Vejamos, por exemplo, o caso do site “Apply Magic Sauce”, utilizado pelo centro de psicometria da universidade de Cambridge para aplicação do estudo de Kosinski, Stilwell e Graepel<sup>5</sup>. Por meio de informações publicamente disponíveis, é possível fazer inferências, com precisão de até 93% de acerto, sobre aspectos íntimos dos usuários da Internet<sup>6</sup>.

Naquele estudo, foram utilizadas as informações sobre as “curtidas” do usuário no *Facebook* – embora, afirmem os autores, possam ser usados quaisquer tipos de dados para alimentar o mesmo mecanismo preditivo – para chegar a conclusões sobre traços de personalidade, sexo, orientação sexual, inteligência, satisfação com a própria vida, idade, área de concentração profissional, opinião política e religiosa, dentre outros.

As correlações, no mundo do *big data*, são infinitas, pois um mesmo conjunto de dados pode ser analisado por algoritmos distintos na busca por novos padrões. Os resultados dessas análises parecem completamente aleatórios em virtude de esses sistemas serem capazes de associar informações em uma escala sem precedentes na história humana.

O *big data*, contudo, depende da coleta massiva de informações. A regra é sempre “quanto mais, melhor”. Os dados sequer precisam ser relevantes no momento da sua coleta, pois a importância surgirá somente depois, com

4 Para uma outra digressão, com outros exemplos, mas com objetivo similar, consultar o debate sobre “The (Occasional) Power of Numbers”, realizado pelo jurista estadunidense Cass R. Sunstein (2006).

5 KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences of the United States of America**, 110, n. 15, 9 abr. 2013. 5802-5805.

6 A maior precisão das análises (93%) refere-se à identificação de uma pessoa como mulher. A orientação sexual tem precisão de 88% para homens e 75% para mulheres.

o processamento por meio do algoritmo adequado. Como resultado da multiplicação desses dispositivos de coleta de dados, será possível falar no surgimento de uma sociedade dos sensores, em que todos os aspectos da vida humana e do meio ambiente tendem a ser mensurados, automaticamente, por dispositivos eletrônicos.

É inquestionável a onipresença de dispositivos capazes de coletar dados sobre o usuário e o ambiente onde estão instalados. Na realidade, a maioria dos equipamentos eletrônicos, embora não possam ser conceituados como sensores exclusivos, desdobram-se como tal. Afinal, a grande maioria dos dispositivos eletrônicos possuem sensores diversos que melhoram a experiência do usuário e agregam novas funções ao equipamento, como é o caso dos giroscópios e sensores de proximidade, de movimento, de luz, de umidade e de campo magnético presentes na maioria dos *smartphones* atuais.

Mesmo no caso de eventos que não sejam imediatamente mensuráveis por um sensor, a utilização do algoritmo certo transforma padrões de uso em informações derivadas mensuráveis. Como exemplo, é possível transformar um telefone celular em um sensor capaz de inferir o humor do usuário. Esse é o caso do *software "MoodScope"*, desenvolvido por um time da Universidade de Houston e o laboratório de pesquisas da Microsoft<sup>7</sup>.

Os dados coletados por esses sensores são imprescindíveis para a compreensão dos modelos preditivos utilizados pela *surveillance*<sup>8</sup>. Esses mecanismos são utilizados, cotidianamente, para realizar análises diversas que geram consequências concretas na vida das pessoas, inclusive com a possibilidade de violação de direitos humanos.

Isso fica claro com a construção de modelos preditivos de risco, seja pela iniciativa privada – como é o caso das análises de risco na concessão de crédito

7 LANE, Nicholas *et al.* MoodScope: building a mood sensor from smartphone usage patterns. **Proceeding of the 11th annual international conference on Mobile systems, applications, and services**. New York: ACM. 2013. p. 389-402.

8 Em síntese, é possível afirmar que os pontos fundamentais que distinguem a "vigilância" do conceito de *surveillance* são: 1) o uso de sentidos estendidos, ou seja, de ferramentas técnicas que expandem a capacidade de coletar informações; 2) a baixa visibilidade de como ocorrem, ou seja, sem que os sujeitos percebam que estão sendo submetidos à coleta de dados; 3) a sua natureza involuntária, uma vez que a *surveillance* está inserida nos aspectos mais triviais da vida humana nas sociedades contemporâneas; 4) a desnecessidade de compartilhamento do mesmo espaço físico, pois a análise de informações pode ocorrer em qualquer lugar com uma conexão de dados e 5) o menor custo associado à obtenção e ao processamento de informações se comparado às tradicionais técnicas de vigilância. JACOB NETO, Elias. Vigilância ou surveillance? Proposta para começar a compreender corretamente este fenômeno. **Revista dos Tribunais**, São Paulo, v. 939, 2014, p. 159-182.



por instituições financeiras, por exemplo –, seja pelo Estado – por exemplo, por meio da análise do risco de que um determinado viajante seja um terrorista. Isso se torna mais grave se for analisado o fato de que, embora extremamente sofisticados, esses modelos preditivos geram resultados falsos. Escondidos sob um manto de suposta neutralidade, tais mecanismos preditivos incorporam os preconceitos dos seus desenvolvedores, o que resulta em erros com consequências drásticas para os direitos humanos.

Esses mecanismos preditivos serão, portanto, analisados sob duas matrizes teóricas. A primeira diz respeito à ideia de simulação e sua vinculação com um modelo pós-pan-óptico de *surveillance*, em virtude da passagem das sociedades disciplinares para as sociedades do controle, o que é viabilizado pelo surgimento das novas tecnologias de informação, que garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos.

A segunda perspectiva de análise irá retornar a Michel Foucault, por meio do conceito de biopoder que, por sua vez, está vinculado à ideia de um Estado que viabiliza o desenvolvimento do capitalismo, por meio do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos. Ao contrário da proposta pan-óptica, o biopoder é exercido de um modo diferente, visto que precisa ser, cada vez mais, dócil.

Por isso, deve garantir a sua manutenção do modo mais assimilável possível, sem causar perturbações ou dificuldades na vida cotidiana, o que torna o biopoder extremamente compatível com o caráter sedutor da *surveillance* na sociedade do consumo. Afinal, a coleta de dados ocorre não nos espaços de opressão, mas de participação e de lazer, como é o caso das redes sociais.

Como resultado, será demonstrado que estamos cada vez mais nos transformando em uma sociedade cujas relações sociais são baseadas em indicadores de confiabilidade, ou seja, saímos da confiança, passamos pelos escores de crédito e caminhamos para os escores sociais, em que os indivíduos passam a ser aquilo que os algoritmos dizem que eles serão no futuro.

## INTRODUÇÃO À SOCIEDADE DOS SENSORES

Se, no passado, a coleta de dados ocorria em “pontos de controle” – ou seja, em determinados momentos, quando se entrava ou saía de um território, por exemplo –, hoje isso ocorre a todo instante. Praticamente todas as atividades – e as “não atividades”, afinal, um telefone celular coleta informações indicando, inclusive, que não está se movendo – do cotidiano geram fluxos de dados individualizados.

Esses dados podem ser reunidos e separados com extrema flexibilidade, conforme demonstra a ideia de *surveillance society*, proposta por David Lyon. Nessa esteira, o autor afirma que,

eventualmente, contudo, somos obrigados a ver que a [surveillance] contemporânea é muito influenciada pelo aparente imperativo de “unir-se”. O desejo de criar assemblages é forte, mesmo que isso não seja sempre acompanhado pela realidade, que pode ser tecnicamente deficiente ou pode encontrar resistência por parte dos usuários, ou ambos. Fluxos separados existem, mas são – ou podem ser – conectados cada vez mais através das redes eletrônicas de informação e comunicação<sup>9</sup>.

Essa coleta de informações oriunda de diversas fontes é viabilizada pela multiplicação de dispositivos que, passivamente, capturam uma vasta gama de dados. A coleta automatizada de dados – como visto no tópico sobre metadados – permite chegar à conclusão de que

[...] a quantidade de dados que um *smartphone* gera sobre o seu usuário em um dia é provavelmente muito superior à quantidade de dados ativamente comunicada pelo seu usuário na forma de mensagens de texto, e-mails e chamadas telefônicas (inclusive porque cada uma dessas atividades gera mais dados sobre elas mesmas: onde o texto foi enviado, qual a duração da chamada, quais websites foram visitados etc<sup>10</sup>).

9 LYON, David. **Surveillance Studies: An Overview**. Cambridge: Polity, 2007. p. 25-26. No original: “Eventually, however, we are obliged to see that contemporary surveillance is very much influenced by the apparent imperative to be joined-up. The desire to create assemblages is strong, even if these are not always matched by the reality, which may be technically deficient or may encounter user resistance, or both. Separate strands do still exist but increasingly, using electronic information and communication networks, they are or can be connected.”

10 ANDREJEVIC, Mark; BURDON, Mark. Defining the Sensor Society. **Television & New Media**, 16, n. 1, jan. 2015. p. 20. DOI: 10.1177/1527476414541552.

Com isso, fica claro que qualquer dispositivo conectado a uma rede de dados, como é o caso dos *smartphones*, pode, também, servir como sensor. Além de gerarem informações sobre o seu uso e sobre o usuário<sup>11</sup>, a maioria desses dispositivos possui diversos sensores que viabilizam suas funções, como é o caso dos giroscópios e sensores de proximidade, de movimento, de luz, de umidade e de campo magnético.

Uma das características desse tipo de coleta de dados é a possibilidade de reutilização dos dispositivos para fins diversos dos originais. Assim, um leitor de livros digitais como o *Kindle* pode, além de permitir o óbvio – a leitura de livros –, coletar informações sobre as preferências literárias do usuário, a sua velocidade de leitura, os fragmentos dos livros que mais interessam, etc.

Essa apreensão do mundo por sensores tem, como finalidade, aquilo que Andrejevic e Burdon chamam de “onisciência diacrônica” Com essa expressão, os autores querem dizer que, quando se reúnem dados suficientes, torna-se possível, além de aplicar algoritmos preditivos do futuro, capturar também o passado. Para eles,

o objetivo da “onisciência diacrônica” é a possibilidade de realizar um arquivo completo capaz de suplementar os inconstantes relatos e memórias através da sua externalização na forma de bancos e dados digitais. [...] Qualquer tentativa de viabilizar a chamada “onisciência diacrônica ” necessariamente acarreta na formação de bancos de dados grandes o suficiente para reduplicar o mundo em formato digital, além da criação de ferramentas capazes de dar sentido a todos esses dados.<sup>12</sup>

No original: “[...] the amount of data that a smart phone generates about its user in a given day is likely to far surpass the amount of data actively communicated by its user in the form of text messages, e-mails, and phone calls (not least because each of these activities generates further data about itself: where the text was sent, how long the call lasted, which websites were visited, and on and on).”

11 As manifestações contra a presidenta da república ocorridas em 13 de março de 2016 contaram, pelo menos na capital paulista, com o uso da tecnologia *SmartLok*, desenvolvida pela *startup* israelense *StoreSmarts*. A partir da quantidade de identificadores únicos emitidos por telefones celulares com tecnologia Wi-Fi ativada, foi possível determinar a quantidade de participantes da manifestação. Segundo entrevista com o dono da empresa, que cedeu “gratuitamente” a tecnologia, Eyal Ben Eliyahu, o mesmo sistema pode ser utilizado de maneira similar para analisar tanto manifestantes políticos, quanto consumidores: “We believe in taking data driven decisions, whether it’s politics or retail. The exposure we get by supporting such requests is very important for us and our partner, as we see Brazil as a very important market”. A matéria de Angelica Mari para o portal *ZDNet* está disponível em: < <http://www.zdnet.com/article/protest-organizers-in-brazil-use-analytics-to-measure-attendance/> >. Acesso em: 10 nov. 2017.

12 ANDREJEVIC, Mark; BURDON, Mark. Defining the Sensor Society p. 30. No original: “The goal of ‘diachronic omniscience’ invokes the possibility of a complete archive that could supplement the vagaries of reported actions and memories by externalizing them in the form of machine-readable databases. [...] Any attempt to approach so-called ‘diachronic omniscience’ necessarily entails the formation of databases

Embora, certamente, faça parte da ideia geral *surveillance society*, a análise da sociedade dos sensores desvia o foco para o desenvolvimento de dispositivos que permitem a coleta e o uso de informações digitais capazes de afetar direitos humanos. Essa perspectiva permite perceber que a tecnologia da informação não é totalmente imaterial, mas depende de estruturas físicas que viabilizam a coleta e a transmissão de dados. Logo, é possível concluir que, por mais líquidas que se considerem, trata-se de tecnologias que dependem de meios físicos para existir, de modo que as relações de propriedade e de controle dessas estruturas são primordiais para a proteção dos direitos humanos.

Os sensores, contudo, apenas coletam e transmitem informações, sem realizar sofisticadas análises. Por isso, a verdadeira violação de direitos humanos ocorre com o uso desses dados em modelos de computador capazes de determinar a probabilidade de ocorrência de um evento por meio de concatenações nada intuitivas que descubrem padrões cujo surgimento é impensável. Trata-se de algo extremamente comum no mundo contemporâneo e que, por isso, merecerá ser tratado minuciosamente no próximo item.

## MODELOS PREDITIVOS DE SURVEILLANCE

A multiplicação de sensores e as análises do *big data* possibilitam o avanço de um campo específico da computação: inteligência artificial, ou, mais especificamente, do que é conhecido como aprendizado de máquinas e aprendizagem profunda – ou *machine learning* e *deep learning* em inglês. Trata-se de áreas do saber cujo objetivo é criar sistemas computacionais capazes de acumular conhecimento, tomando decisões com base nas suas experiências anteriores, realizando análises dos resultados futuros das ações tomadas no presente. Em síntese: sistemas capazes de serem treinados para tomar decisões diante de novos cenários, não apenas para responder face a situações predeterminadas.

Com a coleta de dados do passado, sistemas de computador tomam, no presente, decisões sobre o futuro. É possível afirmar, portanto, que o *big data*

---

large enough to re-duplicate the world in informational form and the development of analytic tools to make sense of these data.”



viabiliza o surgimento de instrumentos que cortam o tempo para muito além da instantaneidade da tecnologia.

Esse é o caso das ferramentas de análise preditivas – *predictive analytics* – que envolvem a criação de modelos de previsão de resultados com base em técnicas de *machine learning*, *deep learning* e *data mining*. Tais técnicas estatísticas analisam padrões em um grande conjunto de dados para realizar previsões dos possíveis cenários futuros, sempre com o objetivo de dar conta da dinâmica do cotidiano.

Dessa maneira, podemos dizer que as análises preditivas são uma tentativa de diminuir as incertezas da modernidade líquida, apostando na alta capacidade de geração e tratamento de dados que, aliados à matemática, seriam capazes de antecipar o futuro. Embora seja adequado dizer que a vida é muito complexa para caber em um algoritmo de computador, esse tipo de análise vem sendo utilizada, cada vez mais, com uma precisão impressionante. Afinal, não importa se a vida cabe ou não em um *bit*, mas se é possível tomar decisões confiáveis com base neles.

Esses mecanismos geram o que pode ser traduzido como “informações utilizáveis” – *actionable intelligence*, no inglês. Essas, por sua vez, são utilizadas

[...] para situar indivíduos em uma matriz de identidades multidimensional e dinâmica. As características destas identidades refletem os interesses dos atores institucionais que buscam influenciar como os indivíduos entendem e respondem às opções que lhe são apresentadas. A apresentação estratégica de opções é feita para maximizar os benefícios e minimizar os riscos associados ao gerenciamento do comportamento destes indivíduos<sup>13</sup>

A finalidade desse tipo de análise, dentro do contexto da *surveillance*, é elaborar formas avançadas de identificação, classificação e avaliação. A primeira das finalidades, a identificação, refere-se ao processo de determinação da identidade dos indivíduos dentro de uma estrutura de poder, diferenciando-os dos demais.

13 GANDY JR., Oscar. Statistical surveillance: Remote sensing in the digital age. In: BALL, Kirsten; HAGGERTY, Kevin; LYON. **Routledge Handbook of Surveillance Studies**. London: Routledge, 2012. p. 125. No original: “[...] to place individuals within a dynamic multidimensional matrix of identities. The character of these identities reflects the interests of the institutional actors seeking to influence how individuals understand and respond to the options that are set before them. The strategic presentation of options is designed to maximize the benefits and minimize the risks that are associated with managing the behavior of these individuals.”

Já a classificação tem como finalidade dizer “o que você é”, ou seja, agrupar distintos indivíduos em virtude de semelhanças compartilhadas entre eles. A tecnologia sob análise é extremamente hábil no reconhecimento de padrões em conjuntos de dados aparentemente desconexos. Essa classificação não necessariamente corresponde à autoclassificação do sujeito, mas às categorias que forem estabelecidas pelo sistema. Como consequência dessa classificação, ocorre também a avaliação, ou seja, a análise preditiva do resultado esperado na interação do indivíduo com o ambiente, com o seu grupo e com outros indivíduos. Nas palavras de David Lyon,

atualmente, dados em massa são obtidos de diferentes fontes e reunidos antes mesmo de determinar os seus usos reais e potenciais e mobilizar algoritmos e análises não só para entender uma sequência de eventos do passado, mas também para prever e intervir antes que comportamentos, eventos e processos ocorram<sup>14</sup>

O fenômeno da *dataveillance*<sup>15</sup> é que conecta o *big data* à *surveillance*, o que ocorre por meio de quatro categorias principais de ação: observação monitorada, identificação e rastreamento, intervenção analítica e modulação de comportamentos<sup>16</sup>.

A primeira categoria diz respeito à multiplicação de dispositivos capazes de coletar informações e armazená-las em formato digital. O tipo mais comum desses dispositivos são as tradicionais câmeras de CFTV. No entanto, em virtude da tendência de computação ubíqua – vejamos, por exemplo, o recente crescimento das aplicações para a “Internet das coisas” –, a coleta de informações por meio

14 LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, 1, n. 2, Jul. 2014. p. 4. No original: “Now bulk data are obtained and data are aggregated from different sources before determining the full range of their actual and potential uses and mobilizing algorithms and analytics not only to understand a past sequence of events but also to predict and intervene before behaviors, events, and processes are set in train.”

15 *Dataveillance* é uma daquelas palavras que seriam impossíveis de traduzir caso se estivesse tratando do fenômeno da *surveillance* como mera vigilância. A tradução mais simples seria “vigilância de dados”, mas isso não traria a real dimensão desse fenômeno. Trata-se da aglutinação das palavras *data* e *surveillance* e pode ser definida como o uso sistemático de sistemas de dados pessoais na investigação e no monitoramento de ações e comunicações de um ou mais indivíduos. A utilização de fluxos de dados discretos oferece um amplo leque de vantagens na análise de pessoas e grupos, já que esse tipo de análise é mais barata; pode ser feita simultaneamente em um número maior de pessoas; é “transparente” ao cotidiano dos indivíduos, ou seja, não é invasiva; ocorre de forma automática e é ubíqua.

16 ESPOSTI, Sara Degli. When big data meets dataveillance: The hidden side of analytics. **Surveillance & Society**, Kingston, 2, n. 12, 2012. P.209-225.

de sensores diversos permite o aumento exponencial de informações coletadas sobre pessoas, objetos e ambientes.

Existe uma tendência na tecnologia atual de embutir sensores em tudo que existe, habilitando que esses dispositivos se comuniquem entre eles. Desde relógios e pulseiras capazes de monitorar a atividade física e o sono do usuário – por todos, ver o *Pebble Watch* e o *Fitbit* – até roupas inteligentes capazes de medir frequência cardíaca e respiratória, bem como intensidade da atividade física, níveis de estresse e calorias gastas – como é o caso da *PoloTech Shirt*, da famosa grife *Ralph Lauren*.

Outro exemplo são os receptores de TV por assinatura da operadora Verizon (EUA) que, em 2012, patenteou<sup>17</sup> um dispositivo capaz de coletar imagens e sons do ambiente e dos telespectadores com a finalidade de oferecer publicidade direcionada para o que estiver acontecendo naquele momento no ambiente monitorado.

Um traço em comum a todos esses dispositivos é que eles possuem conectividade à Internet. Assim, cada um deles cria um fluxo de dados próprio, que é acumulado, processado pelos detentores da tecnologia e outras empresas que conseguem transformar aquelas informações em dinheiro ou poder.

A segunda categoria que conecta o *big data* à *surveillance* é a identificação e o rastreamento, que ocorrem com análise dos traços distintivos de um objeto ou pessoa e à possibilidade de seguir a sua movimentação. A identificação torna-se mais fácil em virtude da proliferação do uso da biometria – para pessoas – ou formas de identificação sem fio para objetos –, como é o caso das etiquetas RFID ou sistemas NFC. Essas categorias são importantes no contexto do *big data*, pois ajudam a resolver os problemas associados aos grandes conjuntos de dados – por meio da sua organização – e aumentam a velocidade de resposta dos sistemas, uma vez que viabilizam a coleta em tempo real de informações.

Exemplos desses sistemas são os controles de fronteiras automatizados

17 A patente descreve um equipamento que permitirá analisar a reação dos usuários à publicidade, “aprendendo” qual o tipo de anúncio desperta o interesse dos telespectadores. O requerimento de patente nº 20120304206 está disponível em < <http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&co1=AND&d=PG01&s1=20120304206&OS=20120304206&RS=2012030420>>. Acesso em: 09 nov. 2017.

– *E-gates* – e passaportes com dispositivos RFID<sup>18</sup>. Em virtude do baixo custo desse tipo de tecnologia, ela vem sendo utilizada pela iniciativa privada em identidades funcionais, como ocorre com cartões de acessos de universidades e empresas. Além de garantirem o acesso ao portador do cartão – identificando-o –, é possível distribuir antenas dentro do ambiente com a finalidade de detectar a exata localização do cartão – tecnologia conhecida como IPS, da sigla em inglês para *indoor positioning system*.

A intervenção analítica, terceira categoria da proposta de Esposti, refere-se à utilização da *analytics* – ou seja, a análise de dados e estatísticas por sistemas digitais com a finalidade de encontrar padrões relevantes – para transformar as informações coletadas em conhecimento útil, isto é, na já mencionada “*actionable intelligence*”<sup>19</sup>, o que ocorre por meio da criação de futuros simulados. Ou seja, é ela que gera a conexão entre o *big data* e a criação de modelos preditivos. Nas palavras de Esposti, o termo *analytics*

indica a análise dos chamados “dados não tratados” na busca de padrões e a consequente transformação destes dados no tipo de conhecimento que os responsáveis pela tomada de decisões necessitam para orientar, de forma otimizada, seu curso de ação.<sup>20</sup>

A intervenção analítica é, na realidade, o principal ponto da compreensão do *big data*. As *analytics* agregam o real valor do *big data*, visto que, sem estes mecanismos, seria como possuir uma enorme biblioteca sem fazer uso dela. Atualmente, são ferramentas bastante utilizadas por entidades públicas e privadas, mas o enfoque principal está no segmento publicitário. Isso porque essas ferramentas permitem, por exemplo, encontrar o preço máximo de um produto que o consumidor está disposto a pagar, maximizando os lucros, ou criar políticas de preços flexíveis para grupos populacionais distintos<sup>21</sup>.

18 Esse sistema verifica a integridade do *chip* RFID do passaporte do viajante, faz uma busca por antecedentes criminais e mandados de prisão em aberto e compara, por meio de biometria, o rosto do viajante com aquele no banco de dados da polícia federal, tudo isso instantaneamente. A matéria completa da Secretaria de Aviação Civil para o Portal Brasil está disponível em: < <http://www.brasil.gov.br/infraestrutura/2016/01/aeroporto-de-campinas-implanta-controle-automatizado-de-passaportes> >. Acesso em: 09 nov. 2017.

19 GANDY JR., Oscar. *Statistical surveillance: Remote sensing in the digital age*. p. 125.

20 ESPOSTI, Sara Degli. *When big data meets dataveillance: The hidden side of analytics*. p. 211-212. No original: “[...] indicates the analysis of so-called ‘raw’ data in search of patterns, and the consequent transformation of these results into the kind of knowledge decision makers need to optimally orientate their course of action [...]”.

21 Em uma pesquisa realizada pelo *Wall Street Journal*, ficou evidente que os preços dos produtos vendidos na *Amazon* variavam conforme o *site* que levou o usuário até a sua página. Assim, consumidores que chegavam até a *Amazon* através de *sites* especializados em descontos pagavam um preço até 23% menor que os demais



É problemático, contudo, acreditar que os resultados desse processamento de dados sejam “verdades matemáticas” – embora sejam derivados do uso da matemática. Os algoritmos de computador não são neutros – possuem erros, vieses e interesses políticos e econômicos –, de modo que o conhecimento derivado desses mecanismos deve ser sempre questionado. Quando eles são incorporados sem a necessária análise, tendem a tomar a forma de manipulação de comportamento, quarta categoria da proposta de Esposti.

A manipulação de comportamento ocorre quando as análises preditivas são transformadas em ações por aqueles que detêm poder para tanto, sempre com a finalidade de modificar um comportamento, geralmente sem consciência daquele que está no polo passivo da relação de poder.

Um dos exemplos mais notórios e polêmicos envolveu um estudo de 2014, realizado por pesquisadores do *Facebook* e da *Cornell University*. Os cientistas conseguiram verificar que o estado emocional das pessoas pode ser manipulado em virtude da exposição delas às emoções de outras pessoas, mesmo sem que ocorra direta interação entre elas. Para demonstrar isso, manipularam o algoritmo de classificação da “linha do tempo” – ou seja, aquilo que é demonstrado para o usuário quando ele entra no *site* – de 689.003 usuários do *Facebook*. De acordo com o estudo,

quando expressões positivas foram reduzidas, as pessoas produziram menos postagens positivas e mais postagens negativas; quando expressões negativas foram reduzidas, ocorreu o padrão oposto. Estes resultados indicam que emoções expressadas por outros no Facebook influenciam nossas próprias emoções, constituindo uma evidência experimental para o contágio em massa através de redes sociais. Este trabalho também sugere que, ao contrário das suposições mais aceitas, o contato pessoal e os sinais não-verbais não são estritamente necessários para o contágio emocional e que a observação das experiências positivas de terceiros constituem uma experiência positiva para as pessoas.<sup>22</sup>

---

usuários. A matéria de Adam Tanner para a revista *Forbes* está disponível em <<https://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/#730bd84b5730>>. Acesso em: 09 nov. 2017.

- 22 KRAMERA, Adam; GUILLORY, Jamie; HANCOCK, Jeffrey. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America*, 2 jun. 2014. p. 8788.

No original: “When positive expressions were reduced, people produced fewer positive posts and more negative

Trata-se de um estudo bastante perturbador, afinal, o *Facebook*, deliberadamente, manipulou as emoções de centenas de milhares de pessoas com o propósito de aumentar os seus lucros por meio do desenvolvimento de algoritmos mais sofisticados de publicidade direcionada. Considerando que tais algoritmos são opacos ao público, que sofre as consequências deles sem ter nenhuma chance de conhecê-los, a manipulação em massa de comportamento por uma empresa privada é, nitidamente, uma violação de direitos humanos.

Por motivos como esses, é necessária cautela quando abordamos, com muito otimismo, a *predictive analytics*, visto que a sua aplicação deve ser analisada, cuidadosamente, sob a perspectiva de proteção dos direitos humanos. Se, por um lado, essas ferramentas podem ser utilizadas para a prestação de um serviço de melhor qualidade, ou mais personalizado, por outro, podem servir para reduzir a capacidade de ação dos indivíduos, visto que solidificam o futuro antes mesmo que ele aconteça – um pouco como no filme *Minority Report*.

Logo, é necessário distinguir entre três tipos principais de algoritmos preditivos. O primeiro tem, como finalidade, desenvolver estratégias para ajudar as pessoas a fazerem escolhas que lhes serão benéficas. O segundo está relacionado à possibilidade de deduzir desejos e traços de personalidade a partir de informações coletadas, como foi o caso da pesquisa de Kosinski et al.<sup>23</sup>, já demonstrada anteriormente. Por fim, o terceiro e mais danoso tipo de algoritmo preditivo é aquele que, como na pesquisa de manipulação de sentimentos dos usuários do *Facebook*, transforma o futuro em presente, restringindo as opções de reação dos indivíduos por meio da sua classificação em categorias distintas.

Esses sistemas preditivos não fazem uma simples coleta ou representação de dados, mas constroem múltiplos tempos – passado, presente e futuro. Eles não simbolizam, necessariamente, uma tendência de desviar a *surveillance* do presente para o futuro, mas uma estratificação do passado e do futuro no presente, criando um presente alternativo que é apresentado como o único possível.

---

posts; when negative expressions were reduced, the opposite pattern occurred. These results indicate that emotions expressed by others on Facebook influence our own emotions, constituting experimental evidence for massive-scale contagion via social networks. This work also suggests that, in contrast to prevailing assumptions, in-person interaction and nonverbal cues are not strictly necessary for emotional contagion, and that the observation of others' positive experiences constitutes a positive experience for people."

23 KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior.

Quando ações preventivas são tomadas com base nesses modelos preditivos, transformamos em verdade um futuro que era apenas uma probabilidade estatística. No entanto, se os direitos humanos são violados para prevenir um possível atentado terrorista, por exemplo, pouco importa se o atentado foi concretizado ou não: o terrorismo já aconteceu, só que patrocinado pelos algoritmos preditivos.

Esse é o caso das listas que o governo estadunidense elabora de pessoas que não podem viajar de avião em virtude de serem potenciais terroristas – as chamadas *no fly lists* –, as quais são construídas por meio de modelos preditivos, cujos critérios são secretos. Um caso específico, por sua peculiaridade, foi muito divulgado pela mídia internacional, pois envolveu um Senador dos EUA sendo classificado como terrorista<sup>24</sup>.

O caso do senador Kennedy demonstra que a precisão não é a maior das prioridades no mundo do *big data*. “Ao invés disto, o seu objetivo é intervir no mundo do modo mais efetivo possível, o que pode implicar em padrões mais baixos de abrangência e precisão”<sup>25</sup>. O problema é que, mesmo sem precisão, tais sistemas são utilizados, cotidianamente, de maneira que afetam a vida das pessoas. Vejamos, por exemplo, os mecanismos de score de crédito, que estão se tornando cada vez mais comuns no Brasil. A partir de uma análise que reúne diversos bancos de dados e variáveis estatísticas – como idade, profissão, local de residência –, esses sistemas atribuem uma “nota” que é utilizada por instituições financeiras e empresas para o cálculo do risco de concessão de crédito. Como resultado, o acesso a um serviço tão importante nos dias de hoje – crédito – depende das análises de algoritmos de computador que permanecem opacos àqueles que têm suas vidas afetadas pelo sistema.

As análises preditivas possibilitam que a criação de categorias como “risco” sejam o resultado de um conjunto complexo de algoritmos que não podem ser

24 Em 2004, o senador estadunidense Edward Kennedy foi impedido de viajar em virtude de “T. Kennedy” ser – de acordo com o algoritmo – um nome falso comumente escolhido por terroristas. Ele, com todas as vantagens políticas do cargo que ocupava, levou cerca de três semanas para inserir na lista a informação de que não era terrorista. Ver a matéria de Gregory Krieg para o jornal *CNN*. Disponível em: < <http://edition.cnn.com/2015/12/07/politics/no-fly-mistakes-cat-stevens-ted-kennedy-john-lewis/> >. Acesso em: 10 nov. 2017.

25 ANDREJEVIC, Mark; GATES, Kelly. Big Data Surveillance: Introduction. *Surveillance & Society*, Kingston, 2, n. 12, 2014. p. 191. No original: “Rather its goal is to intervene in the world as effectively as possible, which may well entail lower standards of comprehensiveness and accuracy.”

explicados de modo tradicional. Isso ocorre porque a complexidade das suas análises não funciona da mesma forma que as deduções do pensamento humano.

As formas de conhecimento que resultam das análises desses algoritmos preditivos são extremamente opacas – embora deixem o indivíduo transparente à análise pelos detentores do poder. Como resultado, “o banco de dados pode gerar padrões que possuem poder preditivo, mas não explicativo”<sup>26</sup>. Podemos afirmar, assim, que o *big data* e as análises preditivas permitem elaborar cenários de aplicação de conjecturas, ou seja, perguntar “e se?”, sem, necessariamente, explicar “como?”<sup>27</sup>.

### SIMULAÇÃO E PÓS-PAN-OPTISMO

As sociedades disciplinares dos séculos XVIII e XIX foram situadas por Foucault<sup>28</sup> no pan-óptico, a partir da ideia de confinamento<sup>29</sup>. Nesse tipo de sociedade, os seres humanos estão sempre transitando entre espaços fechados.

Porém, Deleuze afirma que Foucault sabia da brevidade de prevalência do modelo disciplinar de sociedade, cuja superação ocorreu após a Segunda Guerra Mundial. Além disso, por uma questão de justiça com o autor, cabe ressaltar que o trabalho de Foucault era menos uma análise das sociedades que lhe eram contemporâneas e mais uma obra historiográfica das sociedades do século XVIII e XIX.

Segundo Deleuze, “encontramo-nos numa crise generalizada de todos os meios de confinamento, prisão hospital, fábrica, escola, família”<sup>30</sup>. Essa crise do confinamento, fortalecida, sobremaneira, pela necessidade de mobilidade inerente à globalização, ocorre porque as estruturas das sociedades disciplinares são inflexíveis, incapazes de se adaptar às demandas de um mundo cada vez mais líquido. A distinção entre interior e exterior, necessária para o pleno funcionamento do modelo pan-óptico, é incapaz de absorver a natureza descentralizada das redes de poder típicas da sociedade em rede, o que demanda uma nova forma

26 ANDREJEVIC, Mark; GATES, Kelly. **Big Data Surveillance**: Introduction. p. 186. No original: “The database can generate patterns that have predictive power but not necessarily explanatory power.”

27 ELMER, Greg; OPEL, Andy. Pre-empting panoptic surveillance: surviving the inevitable war on terror. In: LYON, David. **Theorizing Surveillance**: The panopticon and beyond. Cullompton: Willan Publishing, 2006. p. 139-160.

28 FOUCAULT, Michel. **Vigiar e punir**: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

29 DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: DELEUZE, Gilles. **Conversações**. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 219-226.

30 DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. p. 220.



de pensar as novas tecnologias de informação e comunicação (TICs).

Assim, Deleuze explica que os confinamentos são moldes independentes, ou seja, o indivíduo começa do zero a cada passagem de um molde para o outro. Nas sociedades disciplinares, havia sempre recomeços a cada transição dos moldes. Os controles, por sua vez, são modulações autodeformantes, que mudam continuamente<sup>31</sup>. Essa modulação, fazendo uma analogia com o ponto de vista da física, “[...] é o controle variável das características de uma onda. Ela não é aplicada aos indivíduos, mas às oscilações, especificamente, às tendências ou movimentos tendenciais que possuem uma propriedade estatística definida”<sup>32</sup>.

Esse tipo de controle não depende da existência de um interior, ainda que funcione como uma espécie de invólucro. Isso somente se torna factível em virtude do surgimento das TICs, que garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos.

Tal fato que acabamos de afirmar sobre os efeitos no espaço da passagem das sociedades disciplinares para as sociedades do controle também é válido para o tempo. Nas sociedades disciplinares, o confinamento é acompanhado por formas rígidas de controle do tempo de maneira linear. Além disso,

um molde não pode alterar a sua forma, e o objeto que ele produz é fixo. O controle modular adapta-se à desterritorialização das forças produtivas que marca a mudança da organização industrial para a sociedade em rede contemporânea. Ao invés de gerar um objeto fixo, o indivíduo, um invólucro que modula pode variar sua estrutura e o produto que ela produz em resposta às mudanças contingenciais da produção, por exemplo, aquelas geradas pela velocidade e complexidade das comunicações modernas ou o rápido fluxo dos mercados globais<sup>33</sup>.

Em virtude dessa mudança, da disciplina para o controle, Bogard defende que as sociedades do controle necessitam não mais do ideal do pan-óptico, mas do paradigma da simulação de Baudrillard para a sua correta compreensão. O autor explica que as modernas formas de simulação tiveram origem nos métodos estatísticos de amostragem militares, que permitiram a coleta de dados mínimos populacionais com o propósito de prever o seu comportamento futuro.

O trabalho de Bogard deriva das análises de Baudrillard sobre a simulação e o controle pós-pan-óptico. Com efeito, o autor entende que o objetivo máximo da simulação não é refletir a realidade, mas se tornar a realidade. Em suas palavras,

31 DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. p. 221.

32 BOGARD, William. Simulation and post-panopticism. In: BALL, Kirsten; HAGGERTY, Kevin; LYON, David. **Routledge Handbook of Surveillance Studies**. New York: Routledge, 2012. p. 32. No original: “[...] is a variable control over the characteristics of a wave. It is not applied to individuals, but to oscillations, specifically, to ‘trends’ or ‘tendential’ movements that have defined statistical properties [...]”.

33 BOGARD, William. **Simulation and post-panopticism**. p. 33. No original: “A mold cannot alter its form, and the object it produces is fixed. Modulation control adapts to the deterritorialization of productive forces that marks the shift from industrial to network organization in con-temporary society. Rather than generate a fixed object, the individual, an enclosure that modulates can vary its structure and the product it produces in response to changing contingencies of production, for example, those generated by the speed and complexity of modern communications, or the rapid flux of global markets.”

a verdade do signo, a partir de então, é autorreferenciada, não necessitando mais, para a sua verificação, da medida em relação a uma realidade independente. Sistemas de signos constituem a sua própria realidade, ou, como Baudrillard diz, tornam-se 'hiperreaais'<sup>34</sup>

Com base nesse conceito, Bogard estabelece a ideia de *surveillance* simulada ou de *surveillance* como moduladora. Por meio dos mecanismos preditivos de análise de *big data*, a *surveillance* atinge o seu potencial máximo de prever o futuro por meio de sofisticadas simulações capazes de antecipar o maior número possível de contingências. Isso porque, nas sociedades do controle da modernidade líquida, o objetivo dos mecanismos preditivos não é representar a realidade de modo fiel, “[...] mas auxiliar na construção e aplicação de modelos. O que é monitorado, antes de tudo, é a informação sobre a performance do modelo, não os eventos que ele representa”<sup>35</sup>.

A ideia de que os sistemas de análise preditiva – realidades simuladas – derivam de altíssima tecnologia acaba por obscurecer o que eles, de fato, são: modelos especulativos de futuro. Tomar decisões com base nesses sistemas, sob o falso argumento de que suas conclusões são verdades científicas, possui consequências nefastas para os direitos humanos. Por isso, os juristas e os responsáveis pela elaboração de políticas precisam compreender essas ferramentas pelo que elas realmente são: simulações.

## **SURVEILLANCE E NOVO BIOPODER**

Se a proposta pan-óptica de Michel Foucault é amplamente difundida – embora cada vez mais questionada – como paradigma da coleta de informações no mundo contemporâneo, o mesmo não se pode dizer sobre a ideia de biopoder, tema muito menos abordado pela corrente sociológica dos *surveillance studies*. Para Foucault, o biopoder é aquele com a função de gerir a vida, especialmente por meio do exercício de controles reguladores do corpo como processo biológico.

34 BOGARD, William. **Simulation and post-panopticism**. p. 34. No original: “The truth of the sign henceforth is self-referential and no longer needs the measure of an independent reality for its verification. Sign systems constitute their own reality, or as Baudrillard says, they become ‘hyperreal’.”

35 BOGARD, William. **Simulation and post-panopticism**. p. 35. No original: “[...] but to assist in the construction and application of models. What is monitored first of all is information on the performance of the model, and not the event it models.”

Substitui-se, assim, a “potência de morte” do poder soberano do medievo pela gestão calculista da vida por meio de técnicas de controle populacional, as quais se desenvolvem a partir do século XVII. O conhecimento técnico desenvolvido nesse período permitiu as “[...] regulações de população, a demografia, a estimativa da relação entre recursos e habitantes, a tabulação de riquezas e de sua circulação, das vidas com sua duração provável”<sup>36</sup>.

Ainda da análise de Foucault, depreendemos que o biopoder está associado à ideia do Estado, mais especificamente de um Estado que viabiliza o desenvolvimento do capitalismo por meio do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos. Esse poder, no entanto, demanda uma forma de exercício diferente, já que deve ser cada vez mais dócil, ou seja, necessita garantir a sua manutenção do modo mais assimilável possível, sem causar perturbações ou dificuldades na vida cotidiana dos governados.

Ao dissertar sobre o biopoder, Foucault relaciona os dispositivos de segurança ao tratamento do aleatório, que ele considera um dos principais objetivos dos governos liberais<sup>37</sup>. Assim, a finalidade dos dispositivos de segurança é prever a ocorrência de determinados eventos, como é o caso da escassez de alimentos no exemplo utilizado pelo autor.

Por essa razão, é interessante a análise realizada por Ayse Ceyhan<sup>38</sup>. Para ela, a *surveillance* não é apenas uma forma de buscar maior eficiência no controle e gerenciamento de populações por meio da observação e da classificação dos indivíduos, mas, conforme demonstrado no item anterior sobre o *big data* e as *predictive analytics*, é um modo de capturar e controlar as incertezas inerentes à condição humana.

Essa incerteza não é exclusividade dos tempos contemporâneos, visto que a eliminação do incerto foi sempre uma busca humana. Conforme assevera Ceyhan,

36 FOUCAULT, Michel. **História da sexualidade I: a vontade de saber**. Tradução de Meria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 13. ed. Rio de Janeiro: Graal, v. 1, 1998. p. 132.

37 FOUCAULT, Michel. **Segurança Território, População: Curso dado no Collège de France (1997-1978)**. Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008. p. 39/

38 CEYHAN, Ayse. *Surveillance as biopower*. In: BALL, Kirsten; HAGGERTY, Kevin; LYON. **Routledge handbook of surveillance studies**. New York: [s.n.], 2012. p. 38-45.

se, nos tempos de Hobbes, [a incerteza] foi gerada pelas características humanas brutas, como a ganância e o egoísmo, ela é atualmente produzida tanto pelas transformações da modernidade tardia, cujas principais características, conforme Zygmunt Bauman, estão sendo “leve, líquida, móvel, escorregadia” quanto pelas mudanças que ocorrem nos regimes de segurança em virtude das novas formas de violência e a sua disseminação através de redes transnacionais, privadas e virtuais. Essas dinâmicas impactam as alegações de verdade, conhecimento e poder, que já não podem mais contar com os tradicionais marcadores de certeza, como é o caso do território, da hierarquia e da racionalidade que a modernidade tinha definido após o século XVII<sup>39</sup>.

Desde modelos climáticos gerados por computadores de última geração até análises como aquelas do *Google Trends* para gripe e dengue, é possível perceber que, na atualidade, os dispositivos de segurança correspondem às tecnologias capazes de prever os riscos associados ao meio ambiente, à ciência, à tecnologia e à saúde das populações. Assim, “o conceito de aleatório aparece, então, como a variável explanatória que justifica o foco nas tecnologias de gerenciamento de risco que permite a previsão destas mudanças antes delas ocorrerem”<sup>40</sup>.

Diante desse cenário, é possível falar da aplicação da ideia de biopolítica à *surveillance*, já que as informações geradas pelo corpo – por exemplo, identificação biométrica – ou pelo seu movimento – como é o caso da geolocalização de pessoas – são utilizadas na tentativa de domesticar as incertezas, especialmente aquelas relacionadas à segurança do mundo em constante medo<sup>41</sup>.

Isso se deve ao fato do biopoder não precisar ser exercido exclusivamente através do Estado, mas pode partir de qualquer organização que seja capaz de realizar a coleta e o processamento de informações<sup>42</sup>. Com isso, em uma sociedade cuja expansão das tecnologias de informação ocorre de maneira vertiginosa, é possível verificar o surgimento de uma nova modalidade de biopoder, capaz de

39 CEYHAN, Ayse. **Surveillance as biopower**. p. 38. No original: “If in Hobbes’s times it was generated by crude human characteristics like greediness and selfishness, it is now produced both by the transformations of late modernity whose main features, says Zygmunt Bauman, are being “light, liquid, mobile, slippery” and the changes occurring in security regimes by the new forms of violence and their dissemination through transnational, private and virtual networks. These dynamics impact the claims to truth, knowledge and power which no longer rely on the traditional markers of certainty like territory, hierarchy and rationality that modernity had set after the seventeenth century.”

40 CEYHAN, Ayse. **Surveillance as biopower**. p. 40. No original: “The concept of the aleatory appears then as the explanatory variable that justifies the focus on the technologies of risk management that enable the prediction of these changes before they occur.”

41 BAUMAN, Zygmunt. **Medo líquido**.

42 FOUCAULT, Michel. **História da sexualidade I: a vontade de saber**.



[...] desterritorializar e conectar pontos que não foram feitos para serem conectados. Além disso, o poder é agora exercido em locais não tradicionais, como centros de dados, programas de computador e empresas aéreas e telefônicas<sup>43</sup>.

Esse novo biopoder gerencia a vida dos indivíduos de forma eletrônica, por meio de algoritmos desenvolvidos dentro das grandes empresas e sem que haja grande capacidade de intervenção das tradicionais estruturas estatais de regulamentação e controle.

Assim como na perspectiva original de Foucault, a diminuição das incertezas – ou seja, o tratamento do aleatório – depende de procedimentos estatísticos e de cálculos, cujo conhecimento é necessário para o desenvolvimento da força do Estado, até porque, lembra o autor, a própria etimologia da palavra “estatística” remonta à ideia de “conhecimento do Estado”<sup>44</sup>.

A partir da compreensão de que o tratamento da aleatoriedade é uma forma de exercício de poder, concluímos que os mecanismos preditivos associados à *surveillance* podem ser considerados instrumentos para controle da probabilidade e do risco, o que se torna verdade especialmente na sociedade contemporânea, cujas análises preditivas são amplamente utilizadas na tentativa de capturar o futuro antes da sua ocorrência. Essas ferramentas estão fundamentadas na aplicação de técnicas de cálculos probabilísticos e estatísticos, uma das principais características do biopoder de Foucault.

Por outro lado, a globalização e a fluidez da *surveillance* na modernidade líquida modificam a ideia presente em Foucault, motivo pelo qual Ceyhan prefere se referir a uma nova e híbrida forma de biopoder. Embora o biopoder de Foucault esteja fundamentado na regulação de fluxos, as características do mundo contemporâneo modificam o espaço onde esses fluxos ocorrem. Logo,

Não apenas o espaço da mobilidade foi estendido para fora das fronteiras estatais e alcançou o mundo todo, mas ele também se tornou virtualizado e aberto, com a exibição de uma variedade de tecnologias da informação e da comunicação, assim como o desenvolvimento de enormes bancos de dados onde os fluxos de informação são

43 CEYHAN, Ayse. **Surveillance as biopower**. p. 43. No original: “[...] deterritorializes and connects dots which are not in the first place designed to be connected. Moreover, power is now exercised in non-traditional locations like data warehouses, software, airline and phone companies.”

44 FOUCAULT, Michel. **Segurança Território, População**: Curso dado no Collège de France (1997-1978). p. 365.

processados e os dados são extraídos.[...] Isso nos permite definir uma nova forma de governabilidade e poder regulador que está localizado em lugares não tradicionais como a Internet (o Google, por exemplo), shoppings centers, serviços de marketing, companhias telefônicas, empresas e corporações de alta tecnologia.<sup>45</sup>

O exemplo do *Google* é recorrente neste e em outros trabalhos sobre o tema, pois a empresa de *Mountain View* é uma das principais a coletar e analisar grandes volumes de dados sobre pessoas e grupos diversos, sempre com a finalidade de extrair sentido de dados aparentemente desconexos. Uma das subsidiárias do *Google*, denominada “23andme”, por exemplo, permite que a empresa de buscas vá além dos *bits* e possa incorporar, nas suas análises preditivas, os dados genéticos das pessoas. Tal fato permite que a empresa crie diversos modelos de futuro, inclusive, prevendo o aparecimento de características físicas<sup>46</sup> ou doenças.

Assim, essa nova forma de biopoder viabilizada pelas TICs faz parte do que Ceyhan chama de sistema híbrido, ou seja, sistemas “[...] heterogêneos projetados para [a realização] de múltiplas tarefas sem seguir uma direção determinada a priori”<sup>47</sup>. Tais sistemas são fluidos o suficiente para permitirem a sua adaptação às necessidades dos seus desenvolvedores em tempo real, possibilitando a elaboração de modelos preditivos diversos a partir do mesmo conjunto de dados. Esse fenômeno reforça o caráter multifacetado das TICs.

Como resultado, é possível concluir que o modelo de biopoder de Foucault, embora útil, necessita de modificações a fim de poder contribuir para a compreensão da adequação dos mecanismos de análise preditiva na era do *big data*. O biopoder agora é híbrido, vez que congrega uma diversidade enorme de tecnologias, sempre com a finalidade de identificar e rastrear indivíduos e grupos, bem como criar modelos preditivos de comportamento e risco.

45 CEYHAN, Ayse. **Surveillance as biopower**. p. 44. No original: “Not only has the space of mobility been extended outside the state borders and embraced the whole globe, but it has also become virtualized and open-ended with the display of a variety of technologies of information and communication as well as the development of huge databases where flows of information are processed and data mined. [...] This makes us define a new form of governmentality and regulative power that is located in non-traditional places like the Internet (Google, for instance), shopping malls, marketing services, phone companies, businesses and high-tech corporations.”

46 Vejamos, por exemplo, que os dados coletados pelo *23andme* foram utilizados para determinar quais genes contribuem para a calvície masculina. Para mais informações, consultar o estudo completo: LI RIU et al. Six Novel Susceptibility Loci for Early-Onset Androgenetic Alopecia and Their Unexpected Association with Common Diseases. **PLoS Genetics**, San Francisco, v. 2, n. 5. DOI: 10.1371/journal.pgen.1002746.

47 CEYHAN, Ayse. **Surveillance as biopower**. p. 44. No original: “[...] heterogeneous systems designed for multiple tasks implemented without following an overarching direction from the beginning.”

**CONSIDERAÇÕES FINAIS**

Pelo exposto, deve ter ficado claro que os algoritmos de análise preditivas – *predictive analytics* – são amplamente empregados como forma de diminuir as incertezas na sociedade securitizada. Por meio de cálculos probabilísticos complexos, essa tecnologia busca antecipar o futuro para gerar respostas – sejam elas políticas, jurídicas, econômicas ou militares – antes mesmo que o potencial evento danoso aconteça.

A análise desses mecanismos e a compreensão das modificações nas relações de tempo que eles proporcionam fazem sentido somente se for considerado, como defendido neste artigo, que houve a superação da sociedade disciplinar em direção às sociedades do controle. Ultrapassamos, assim, a necessidade de confinar aqueles que necessitam ser controlados. A flexibilidade e a ubiquidade da tecnologia da informação garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos – contêineres territoriais.

Ao encontro dessa tendência de calcular os riscos com a finalidade de prever o futuro está a ideia de biopoder, que viabilizou o desenvolvimento do capitalismo por meio do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos. O biopoder é exercido de um modo oposto à proposta pan-óptica, visto que ele precisa ser cada vez mais dócil, proporcionando sempre a sensação de liberdade. Para tanto, deve garantir a sua manutenção do modo mais assimilável possível, sem causar perturbações ou dificuldades na vida cotidiana.

Esse traço torna o modelo do biopoder extremamente compatível com o caráter sedutor das TICs na sociedade do consumo, sobretudo se for atualizado, a fim de poder contribuir para a compreensão da *surveillance* na era do *big data*. O biopoder agora é híbrido, congregando um amplo leque de tecnologias distintas, sempre com a finalidade de identificar e rastrear indivíduos e grupos, bem como criar modelos preditivos de comportamento e risco.

Sejam públicas ou privadas, todas as entidades que coletam e analisam dados, na atualidade, possuem em comum a busca pela categorização e pelo

reconhecimento de padrões – *data mining* – em enormes conjuntos de dados – *big data*. Isso decorre da transição do modelo da defesa em direção à atual sociedade securitizada, na qual o medo líquido preenche as vidas de incertezas que precisam ser eliminadas a partir de novas tecnologias.

Essa securitização, para utilizar a expressão de Michael Hardt e Antonio Negri<sup>48</sup>, modifica a expectativa de resposta dos sistemas tecnológicos, que deixam de ser reativos e conservativos – ou seja, preservar a ordem por meio de interferências somente quando perturbados –, para se tornarem ativos e construtivos – antecipar essas interferências e modificar a ordem social antes mesmo que elas ocorram.

Como resultado, esse fenômeno enfraquece a soberania moderna em virtude da sua capacidade para normalizar uma situação de guerra constante, que deveria ser excepcional. Como resultado, desestabiliza-se o poder, que passa a migrar em direção aos atores públicos – vinculados às grandes potências – e privados – detentores da tecnologia da informação. Tal situação é extremamente importante para a consideração dos juristas, uma vez que coloca em risco o modelo democrático e os direitos fundamentais. Na sociedade contemporânea, o “pré-crime”, presente no filme *Minority Report*, já não é tão ficção assim.

## REFERÊNCIA DAS FONTES CITADAS

ANDREJEVIC, Mark; BURDON, Mark. Defining the Sensor Society. *Television & New Media*, 16, n. 1, jan. 2015. 19-36. DOI: 10.1177/1527476414541552.

ANDREJEVIC, Mark; GATES, Kelly. *Big data* Surveillance: Introduction. *Surveillance & Society*, Kingston, 2, n. 12, 2014. 185-196.

BAUMAN, Zygmunt. Medo líquido. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2008. 239 p.

BOGARD, William. Surveillance assemblages and lines of flight. In: LYON, David. *Theorizing surveillance: the panopticon and beyond*. Cullompton: Willan Publishing, 2006. p. 97-122.

48 HARDT, Michael; NEGRI, Antonio. Globalization as Empire. In: HELD, D; MCGREW, A. *The Global Transformations Reader: An Introduction to the Globalizing Debate*. 2. ed. Cambridge: Polity, 2003. p. 116-119.



BOGARD, William. Simulation and post-panopticism. In: BALL, Kirsten; HAGGERTY, Kevin; LYON, David. Routledge Handbook of Surveillance Studies. New York: Routledge, 2012. p. 30-37.

CEYHAN, Ayse. Surveillance as biopower. In: BALL, Kirsten; HAGGERTY, Kevin; LYON. Routledge handbook of surveillance studies. New York: [s.n.], 2012. p. 38-45.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: DELEUZE, Gilles. Conversações. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 219-226.

ELMER, Greg; OPEL, Andy. Pre-empting panoptic surveillance: surviving the inevitable war on terror. In: LYON, David. Theorizing Surveillance: The panopticon and beyond. Cullompton: Willan Publishing, 2006. p. 139-160.

ESPOSTI, Sara Degli. When *big data* meets dataveillance: The hidden side of analytics. Surveillance & Society, Kingston, 2, n. 12, 2012. 209-225.

FOUCAULT, Michel. História da sexualidade I: a vontade de saber. Tradução de Meria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 13. ed. Rio de Janeiro: Graal, v. 1, 1998. 152 p.

FOUCAULT, Michel. Vigiar e punir: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

FOUCAULT, Michel. Segurança Território, População: Curso dado no Collège de France (1997-1978). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008. 572 p.

GANDY JR., Oscar. Statistical surveillance: Remote sensing in the digital age. In: BALL, Kirsten; HAGGERTY, Kevin; LYON. Routledge Handbook of Surveillance Studies. London: Routledge, 2012. p. 125-132.

GRAHAM, Stephen. Cities under siege: the new military urbanism. London: Verso, 2010. 402 p.

HARDT, Michael; NEGRI, Antonio. Globalization as Empire. In: HELD, David; MCGREW, Anthony. The Global Transformations Reader: An Introduction to the Globalizing Debate. 2. ed. Cambridge: Polity, 2003. p. 116-119.

JACOB NETO, Elias. Vigilância ou surveillance? Proposta para começar a compreender corretamente este fenômeno. Revista dos Tribunais, São Paulo, v. 939, 2014, p. 159-182.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences of the United States of America, 110, n. 15, 9 abr. 2013. 5802-5805.

KRAMERA, Adam; GUILLORY, Jamie; HANCOCK, Jeffrey. Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences of the United States of America, 2 jun. 2014. 8788-8790.

LANE, Nicholas *et al.* MoodScope: building a mood sensor from smartphone usage patterns. Proceeding of the 11th annual international conference on Mobile systems, applications, and services. New York: ACM. 2013. p. 389-402.

LI RIU et al. Six Novel Susceptibility Loci for Early-Onset Androgenetic Alopecia and Their Unexpected Association with Common Diseases. PLoS Genetics, San Francisco, v. 2, n. 5. DOI: 10.1371/journal.pgen.1002746

LYON, David. Surveillance Studies: An Overview. Cambridge: Polity, 2007. 243 p.

LYON, David. Surveillance, Snowden, and *Big data* : Capacities, consequences, critique. *Big data & Society*, 1, n. 2, Jul. 2014. 1-13. DOI: 10.1177/2053951714541861.

SALTER, Mark. The global visa regime and the political technologies of the international self: borders, bodies, biopolitics. *Alternatives*, 31, n. 2, abr. 2006. 167-189. DOI: 10.1177/030437540603100203.

SUNSTEIN, Cass. Infotopia: How Many Minds Produce Knowledge. New York: Oxford University Press, 2006. 273 p.



Recebido em: novembro/2017

Aprovado em: março/2018